UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/613,636	07/03/2003	Bhargava K. Yenduri	SUNMP459	4610

32291 7590 01/15/2008
MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
01/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

D

Advisory Action Before the Filing of an Appeal Brief	**Application No.** *10/613,636*	**Applicant(s)** YENDURI, BHARGAVA K.	
	Examiner Farid Homayounmehr	**Art Unit** 2132	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 19 December 2007 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. □ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires 2 months from the mailing date of the final rejection.

b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. □ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) □ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) □ They raise the issue of new matter (see NOTE below);
   (c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) □ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. □ Applicant's reply has overcome the following rejection(s): _____.
6. □ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) □ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1,3,9-11,25,27,29 and 30*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. □ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. □ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. □ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____
13. □ Other: _____.

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Continuation of 11. does NOT place the application in condition of allowance because applicant's argument is not persuasive:

Applicant argues that Rowland's Loadable Kernel Module Agent 1306 only looks for kernel modules and does not verify them. However, as indicated in parag. 149, said agent looks for known and unknown kernel modules. It looks for Modified kernel modules. The agent must verify the modules to determine it they are modified or not. Parag. 149 clearly sates that the modified kernel modules are created and loaded by attackers. Unless the applicant contends that the attacker labels the modified module so it can be detected by looking for it, the agent must verify the module to see if it is modified. In addition, the Final rejection points out that paragraph 148 teaches a Known Intrusion Agent 1305, which uses signatures to identify intrusions such as suspect loadable kernel modules. The rejection further explains that agents 1306 and 1305 are part of a group called Mobile Autonomous Code (MAC) Security Agents. Therefore, Rowland teaches a system (agents) that look for and verify kernel modules, as required by the claim.

Applicant further argues: "Furthermore, the Loadable Kernel Module Agent looks for LKMs that are already loaded, that is quite different from verifying said kernel module signature information when said plurality of kernel modules are loaded. Verifying a kernel module before being loaded protects the system from malicious kernel modules being loaded, but Rowland only teaches how to look for modules that have already been loaded in compromised systems in order to take corrective action." However, it is not clear why the applicant assumes that Rowland's system is limited to verifying modules only after they are loaded in the <u>kernel</u>. Clearly, to verify the module, it must be first loaded somewhere in the system. The question is, if the verification is performed before the kernel module is loaded into the kernel or after that. First, applicant's claim 1 never explicitly requires verifying the kernel modules <u>before</u> they are loaded in <u>the kernel</u>. Second, even if it is assumed that the claims intend to verify before loading into the kernel, Rowland also teaches verification before loading to prevent attacks. Cited paragraph 148 clearly indicates that the Known Intrusion Agent is designed to roam the network and detect activity <u>before</u> it becomes widespread. Therefore, this agent verifies loadable kernel modules, and stops them before they affect systems. Note that paragraph148 identifies suspicious loadable kernel modules as one of the types of files whose signature is verified to detect potential problems.

Applicant further argues that the meaning of the word signature is misinterpreted. Applicant compares the meaning of a "digital signature" and a "signature" and argues that what Rowland relies on is a "signature" and not a "digital signature", as it is used by the claim language. Applicant underlines a portion of paragraph 148 in an attempt to indicate that Rowland uses signatures and not digital signatures. However, paragraph 148 is not limited to signatures of Trojan Horses. Paragraph 148 clearly lists suspicious loadable kernel modules as one of the types of suspicious files detected by the system. Applicant admits that digital signatures are key components of authentication schemes. In addition Rowland teaches use of digital signatures in authenticating files and identifying modified files. Examples are in paragraph 131-133, 151 and more particularly paragraph 146. Therefore, Rowland teaches using digital signatures to verify the integrity of a file, including a loadable kernel module.

With respect to Examiner's Official Notice, stating that use of public and private keys to create signature verification protocol is well known in the art, applicant argues that the use of kernel module signature information is not well-known in the art. However, as described above, and in the Final Rejection, the use of signatures <u>to identify kernel modules</u> is shown by Rowland. Examiner's Official Notice is about the <u>use of public and private keys in performing signature verification</u>. Applicant further refers to MPEP 2144.03, stating that if the applicant traverses an Official Notice, the examiner should cite a reference. However, per section "C" of MPEP 2144.03: "To adequately traverse such a finding, an applicant must <u>specifically</u> point out the supposed errors in the examiner's action, which would include stating <u>why the noticed fact is not considered to be common knowledge or well-known in the art."</u> Applicant's challenge merely includes a statement that the use of kernel module signature information is not well-known in the art. More particularly, there is no discussion supporting that <u>use of public and private keys in performing signature verification</u> is not well-known in the art. Therefore, applicant's argument amounts to a general allegation, and a general allegation that the claims define a patentable invention without any reference to the examiner's assertion of official notice would be inadequate. The common knowledge or well-known in the art statement is taken to be admitted prior art because applicant's traverse is inadequate.

Applicant further argues that because Rowland's MAC agents travel in the network, so they cannot be kernel modules. However, applicant is claiming a system for verifying the kernel modules. Rowland's MAC agents are systems that verify kernel modules. In addition, the invention and Rowland's teaching are about <u>loadable</u> kernel modules. Loadable kernel modules are not an inseparable part of the kernel, as they are loaded to the kernel prior to the start of their functionality. Rowland's agents also travel in the network, but they are eventually loaded in the system were they perform their functionalities (see for example figs 11 and 12). To perform within an environment, the agent must match the execution environment of the host (the client or the server where the agent is loaded). Therefore, applicant's argument that an agent cannot suggest a kernel cryptographic framework, because it travels in the network, or fits the host's execution environment is not persuasive.

Applicant's last argument is based on their initial argument that verifying a module is different than looking for a file. However, as explained in the above, Rowland teaches verifying a module as required by the claim.

Based on the discussion above, applicant's argument is found non persuasive, and the rejections are maintained.